1984

Maximal ternary codes and Plotkin's bound

Conrad Mackenzie

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Abstract

The analogue of Plotkin's bound is developed for ternary codes with high distance relative to length. Generalized Hadamard matrices are used to obtain codes which meet these bounds. The ternary analogue of Levenshtein's construction is discussed and maximal codes constructed.

Publication Details

Mackenzie, C and Seberry, J, Maximal ternary codes and Plotkin's bound, Ars Combinatoria, 17A, 1984, 251-270.

Maximal Ternary Codes and Plotkin's Bound

Conrad Mackenzie and Jennifer Seberry*

Department of Applied Mathematics

University of Sydney

N.S.W., 2006 Australia

The analogue of Plotkin's bound is developed for ternary codes with high distance relative to length, obtaining

$$A(n,d) \le 3\left[\frac{d}{3d-2n}\right] \qquad 3d > 2n\ ,$$

$$A(n,2n/3) = 3n \qquad 3d = 2n\ .$$

Generalized Hadamard matrices are used to obtain codes which meet these bounds. The ternary analogue of Levenshtein's construction is discussed and maximal codes constructed.

The Plotkin bound.

Let A be the $M \times n$ matrix whose rows are the codewords of a ternary code, C. Suppose the ith column of A contains x_i 0's, y_i 1's, z_i 2's. Following the method of Plotkin we calculate the sum

$$\sum_{u \in C} \sum_{v \in C} \operatorname{dist}(u,v)$$

in two ways. Since dist $(u,v) \ge d$ if $u \ne v$, the sum is $\ge M(M-1)d$. But each column of A contributes

$$2x_i y_i + 2y_i z_i + 2z_i x_i, \qquad x_i + y_i + z_i = M$$

* Research supported by a grant from the Australian Computer Research Board.

ARS COMBINATORIA, VOL. 17A (1984), pp. 251-270

to the above sum. Hence summing over all columns we have

$$S = \sum_{i=1}^{n} (2x_i y_i + 2y_i z_i + 2z_i x_i) \geq M(M-1)d .$$

We use Lagrange multipliers to maximize

$$S + \Sigma\lambda_i (x_i + y_i + z_i - M)$$

and find the maximum occurs when $x_i = y_i = z_i = M/3$ and so if

a) $M \equiv 0 \pmod 3$ we have

$$M(M-1)d \leq 2M^2 n/3$$

$$M \leq \frac{3d}{3d-2n}$$

and since $3|M$ we have

$$M \leq 3\left[\frac{d}{3d-2n}\right] \quad \text{for} \quad 3d > 2n . \tag{1}$$

b) $M = t+3s$, $t \neq 3$, the maximum occurs when t of x_i, y_i, z_i are $s+1$ and $3-t$ are s and so

$$M(M-1)d \leq n\left(4s(s+1) + 2(s+t-1)^2\right) .$$

Now $t = 1$ gives $\quad 3s(3s+1)d \leq 2ns(3s+2)$

or $\quad s \leq \frac{4n-3d}{9d-6n}$ as $s \geq 0$

and as $M \equiv 1 \pmod 3$

$$M \leq 3\left[\frac{4n-3d}{9d-6n}\right] + 1 \quad \text{for} \quad 3d > 2n.$$

Also $t = 2$ gives $\quad (3s+2)(3s+1)d \leq 2n(3s+1)(s+1)$

or $\quad s \leq \frac{2n-2d}{3d-2n}$ as $3s+1 \geq 0$

and as $M \equiv 2 \pmod 3$

$$M \le 3\left[\frac{2n-2d}{3d-2n}\right] + 2$$

$$\le 3\left[\frac{d}{3d-2n}\right] - 1 \qquad \text{for} \quad 3d > 2n .$$

c) If $2n = 3d$ we have $M = 3n$.

Summarizing, we have, noting (1) is larger than the other bounds:

THEOREM 1. *For an alphabet of* 3 *symbols, the maximum number of codewords of length* n *and distance* d, A(n,d), *satisfies*

$$A(n,d) \le 3\left[\frac{d}{3d-2n}\right] \qquad \textit{for} \quad 3d > 2n \ge 2d . \tag{2}$$

This result is given by Blake and Mullin (p 85) but also

LEMMA 1. $A(n,d) \le 3A(n-1,d)$.

Proof. Given a ternary (n,M,d) code, the codewords fall into three classes, those beginning with 0, 1 and 2. One class must contain at least one third of the codewords, thus

$$A(n-1,d) \ge A(n,d)/3 .$$

This gives us

THEOREM 2. (i) $A(3n,2n) \le 9n$.

(ii) $A(3n+1,2n+1) \le 6n+3$.

(iii) $A(3n+1,2n) \le 27n$.

(iv) $A(3n-1,2n) \le 3n$.

Proof. (i) $A(3n,2n) \le 3A(3n-1,2n) \le 3.3\left[\frac{2n}{6n-2(3n-1)}\right] = 9n$.

(ii) $A(3n+1,2n+1) \le 3\left[\frac{2n+1}{3(2n+1)-2(3n+1)}\right] = 6n+3$.

(iii) $A(3n+1,2n) \le 3A(3n,2n) = 27n.$

(iv) $A(3n-1,2n) \le 3\left[\frac{2n}{6n-2(3n-1)}\right] = 3n.$

To construct maximal ternary codes we require some lemmas concerning generalized Hadamard matrices of the form $GH(n,Z_3)$. This paper will not discuss the theory of generalized Hadamard matrices, nor their existence or non existence. However the following definitions and lemmas are required.

A square matrix of size n with entries from a group G is called a *generalised Hadamard matrix*, $GH(n,G)$, if the inner product of any two distinct rows, $\underset{\sim}{a} = (a_1,\ldots,a_n)$, $\underset{\sim}{b} = (b_i,\ldots,b_n)$, $a_i, b_j \in G$, defined by $\underset{\sim}{a}\cdot\underset{\sim}{b} = \sum_{i=1}^{n} a_i b_i^{-1}$ is $n/|G|$ copies of G. For example we have

$$GH(3,Z_3) \qquad \begin{pmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{pmatrix}$$

$$GH(6,Z_3) \qquad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & w & w^2 & w^2 & w \\ 1 & w & 1 & w & w^2 & w^2 \\ 1 & w^2 & w & 1 & w & w^2 \\ 1 & w^2 & w^2 & w & 1 & w \\ 1 & w & w^2 & w^2 & w & 1 \end{pmatrix}$$

The results of de Launey, Drake, Jungnickel, Rajkundlia, Seberry, Seiden and Street allow us to say:

LEMMA 2. *There exist* $GH(n,Z_3)$ *for*

(i) $n=3^t$, (ii) $n=6$, (iii) $n=12$, (iv) 2.3^t, (v) 4.3^t. *A* $GH(n,Z_3)$ *does not exist for* $n=15$. $n=21$ *is undecided*.

Any $GH(n,Z_3)$ *is equivalent to a* $GH(n,Z_3)$ *with its first row and column consisting entirely of the unit element of the group.*

LEMMA 3. *A* $GH(n,Z_3)$ *gives block codes over a 3-symbol alphabet with parameters,* (n,M,d):

(i) (n,3n,2n/3), (ii) (n-1,3n,2n/3-1), (iii) (n-1,n,2n/3), (iv) (n-2,n,2n/3-1).

LEMMA 4. *The following codes exist over a 3-symbol alphabet:*

(i) (4,9,3), (ii) (5,18,3), (iii) (8,17,5).

(4,9,3)

0	0	0	0
0	1	2	1
0	2	1	2
1	1	1	0
1	2	0	1
1	0	2	2
2	2	2	0
2	0	1	1
2	1	0	1

(5,18,3)

0	0	0	0	0
0	1	2	2	1
1	0	1	2	2
2	1	0	1	2
2	2	1	0	1
1	2	2	1	0
1	1	1	1	1
1	2	0	0	2
2	1	2	0	0
0	2	1	2	0
0	0	2	1	2
2	0	0	2	1
2	2	2	2	2
2	0	1	1	0
0	2	0	1	1
1	0	2	0	1
1	1	0	2	0
0	1	1	0	1

(8,17,5)

0	0	0	0	0	0	0	0
2	2	2	2	2	2	2	1
1	1	1	1	1	1	1	2
1	2	2	0	2	0	0	2
0	1	2	2	0	2	0	2
0	0	1	2	2	0	2	2
2	0	0	1	2	2	0	2
0	2	0	0	1	2	2	2
2	0	2	0	0	1	0	2
0	2	0	2	0	0	1	2
2	1	1	0	1	0	0	1
0	2	1	1	0	1	0	1
0	0	2	1	1	0	1	1
1	0	0	2	1	1	0	1
0	1	0	0	2	1	1	1
1	0	1	0	0	2	1	1
1	1	0	1	0	0	2	1

A number of authors including de Launey, Lam, Seberry and Street and Rodger have studied an extension of generalized Hadamard matrices in which the elements are over a group ring, called Bhaskar Rao designs (BRD). Since we are concerned with ternary codes we restrict ourselves to the group ring $\{0\}+Z_2$. A *Bhaskar Rao design* $W = A - \dot{B}$ with parameters v,b,r,k,λ satisfies

$$
\begin{aligned}
WW^T &= rI_v \\
(A+B)(A+B)^T &= (r-\lambda)I + \lambda J \\
J(A+B) &= kJ,\ (A+B)J = rJ,
\end{aligned}
$$

where A, B are $(0,1)$-matrices, $A+B$ is a $BIBD(v,b,r,k,\lambda)$. The BRD is written $BRD(v,b,r,k,\lambda;Z_2)$ or $BRD(v,k,\lambda)$ for brevity. Such designs can be extended to partially balanced and pairwise balanced designs and to groups other than Z_2.

In the remainder of this section we use

$$
\begin{aligned}
r &= \lambda(v-1)/(k-1) \\
b &= vr/k,
\end{aligned}
$$

and if $W = A - B$ is a BRD where $AJ = JA = k_1J$, $BJ = JB = k_2J$

$$
\begin{aligned}
k &= k_1 + k_2, \\
\lambda(v-1)/2 &= k_1(k_1-1) + k_2(k_2-1).
\end{aligned}
$$

LEMMA 5. *If there exists a* $BRD(v,b,r,k,\lambda)$ *then there exist* 3-*symbol codes with parameters*

(i) $(vr/k, v, 2r-3\lambda/2)$,

(ii) $(vr/k, v+3, \min(2r-3\lambda/2, b-k_1, b-k_2, b-r))$,

(iii) $(vr/k, 2v, \min(r, 2r-3\lambda/2))$.

Proof. Let M be the BRD. The result follows by considering the rows of

$$M\ , \qquad \begin{bmatrix} 0 & \dots & 0 \\ 1 & \dots & 1 \\ - & \dots & - \\ & M & \end{bmatrix}\ , \quad \begin{bmatrix} M \\ \\ -M \end{bmatrix}$$

respectively as codewords.

Corollary 6. *Since there exist* BRD(7,4,2), BRD(13,9,6), BRD(19,9,4), BRD(21,16,12), BRD(8,28,14,4,6) *and* BRD(13,26,8,4,2) *there exist* (7,7,5), (7,10,5), (7,14,4), (13,26,9), (19,19,12), (19,38,9), (21,21,14), (21,42,14), (28,8,19), (28,16,14), (26,13,13), (26,26,8) codes.

LEMMA 7. *If there exists a regular (= constant row sum)* BRD(v,k,λ) *then there exist 3-symbol codes with parameters* $(vr/k, 3v, \min(2r-3\lambda/2, x_1+b-2r+2\lambda, -x_1+b-\lambda/2)$ *where* x_1 *is the number of occurrences of* $\begin{Bmatrix} 0 \\ 1 \end{Bmatrix}$ *and* $0 \le x_1 \le r-\lambda$. *The regular cyclic* BRD(t^2+t+1, t^2, t^2-t) *give* $\left(t^2+t+1, 3(t^2+t+1), \tfrac{1}{2}(t^2+t+2)\right)$*-codes*.

Proof. Let M be the BRD and consider

$$\begin{bmatrix} M \\ M+1 \\ M+2 \end{bmatrix} .$$

Any two rows of this code, $\underset{\sim}{a}$, $\underset{\sim}{b}$, can be written as

$$\begin{array}{ccccccccccccccccc} \underset{\sim}{a} & = & 0 & & \dots\dots & & 01 & & \dots\dots & & 12 & & \dots\dots & & 2 \\ \underset{\sim}{b} & = & \multicolumn{13}{l}{1\dots12\dots20\dots01\dots12\dots20\dots01\dots12\dots20\dots0\ .} \\ & & x_1 & y_1 & z_1 & & x_2 & y_2 & z_2 & & x_3 & y_3 & z_3 \end{array}$$

Without loss of generality we assume $k_1 \ge k_2$. Now $k_1 = x_2+y_2+z_2 = x_1+x_2+x_3$ (1), $k_2 = x_3+y_3+z_3 = y_1+y_2+y_3$ (2), $r = k_1+k_2$ (3) assuming regularity of rows. Now the fact that the rows of the BRD (when considered as $0, \pm1$) are orthogonal means

$$x_2 + y_3 = y_2 + x_3 = \frac{\lambda}{2} \tag{4}$$

and we have
$$x_1 + y_1 = r - \lambda = z_2 + z_3 , \tag{5}$$

$$z_1 = b - 2r + \lambda . \tag{6}$$

Considering $\underset{\sim}{a}, \underset{\sim}{b}, \underset{\sim}{b}+\underset{\sim}{1}$ and $\underset{\sim}{b}+\underset{\sim}{2}$ as codewords we want the minimum of the distances $d_1 = d(\underset{\sim}{a},\underset{\sim}{b})$, $d_2 = d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{1})$, $d_3 = d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{2})$ over all $\underset{\sim}{a},\underset{\sim}{b}$ in the code. Now

$$d_1 = x_1+y_1+y_2+z_2+x_3+z_3 = 2(x_1+y_1)+y_2+x_3 = 2r-3\lambda/2$$

$$d_2 = x_1+z_1+x_2+y_2+y_3+z_3 = x_1+z_1+\lambda = x_1+b-2r+2\lambda$$

$$d_3 = y_1+z_1+x_2+z_2+x_3+y_3 = 2b-d_1-d_2 = -x_1+b-\lambda/2 .$$

Hence distance of code is $\min(2r-3\lambda/2, x_1+b-2r+2\lambda, -x_1+b-\lambda/2)$ where $0 \le x_1 \le \min(k_1, r-\lambda)$ is the number of occurrences of $\begin{pmatrix}0\\1\end{pmatrix}$.

In particular for cyclic $BRD(t^2+t+1, t^2, t^2-t)$ the minimum distance is $\frac{1}{2}(t^2+t+2)$. □

<u>Corollary 8</u>. *There exist* (7,21,4),(13,39,7),(19,57,12) and (21,63,11) *codes.*

Codes for which $3d \ge 2n \ge 2d$

n	M(found)	M(max)	d	Construction or Comment
3	9	9	2	Lemma 3 (i),
4	9	9	3	Lemma 4 (i),
5	6	6	4	Lemmas 1 and 3 (iii),
6	18	18	4	Lemma 3 (i),
7	10	15	5	Corollary 6,
8	9	9	6	Lemmas 1 and 2 (iii),
9	27	27	6	Lemma 3 (i),
9	6	6	7	(4,9,3) + (5,6,4),
10	12	18	7	From (11,12,8), Lemma 1,
10	6	6	8	(5,6,4) +(5,6,4),

11	12	12	8	Lemmas 1 and 3 (iii),
12	36	36	8	Lemma 3 (i),
12	9	9	9	(4,9,3) + (8,9,6),
13	13	27	9	Corollary 6,
14	9	15	10	(6,18,4) + (8,9,6), Lemma 1,
15	18	45	10	(6,18,4) + (9,27,6),
15	9	11	11	Lemma 1, (7,10,5) + (8,9,6),
16	18	33	11	From (17,18,12)
17	18	18	12	Lemma 3 (iii),
18	54	54	12	Lemma 3 (i)
18	9	12	13	(8,9,6) + (10,12,7),
19	12	36	13	(10,12,7) + (9,27,6), Lemma 1
20	12	21	14	(9,27,6) + (11,12,8),
21	42	63	14	Corollary 6.

Table 1.

A property of ternary codes used to give more codewords

LEMMA 9. *Let* $\underset{\sim}{a}$ *and* $\underset{\sim}{b}$ *be two ternary vectors. Then*

$$d(\underset{\sim}{a},\underset{\sim}{b}) + d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{1}) + d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{2}) = 2n$$

$$d(\underset{\sim}{a}+\underset{\sim}{i},\underset{\sim}{b}+\underset{\sim}{j}) = d(\underset{\sim}{a}+\underset{\sim}{i}+\underset{\sim}{k},\underset{\sim}{b}+\underset{\sim}{j}+\underset{\sim}{k}),\ \underset{\sim}{i},\underset{\sim}{j},\underset{\sim}{k} \in \{\underset{\sim}{0},\underset{\sim}{1},\underset{\sim}{2}\}\ .$$

Proof. The second part of the lemma is obviously true for linear codes but we show it is also true for block codes. We write the two codewords as

$$\begin{array}{lcl} \underset{\sim}{a} & = & 0 \;\ldots\ldots\; 01 \;\ldots\ldots\; 12 \;\ldots\ldots\; 2 \\ \underset{\sim}{b} & = & 0\ldots01\ldots12\ldots20\ldots01\ldots12\ldots20\ldots01\ldots12\ldots2 \\ & & \quad x_{00} \quad x_{01} \quad x_{02} \quad x_{10} \quad x_{11} \quad x_{12} \quad x_{20} \quad x_{21} \quad x_{22} \end{array}$$

$$\begin{array}{rcl} \text{Now}\quad d(\underset{\sim}{a},\underset{\sim}{b}) & = & x_{01}+x_{02}+x_{10}+x_{12}+x_{20}+x_{21} = d(\underset{\sim}{a}+\underset{\sim}{1},\underset{\sim}{b}+\underset{\sim}{1}) = d(\underset{\sim}{a}+\underset{\sim}{2},\underset{\sim}{b}+\underset{\sim}{2}) \\ d(\underset{\sim}{a}+\underset{\sim}{1},\underset{\sim}{b}) & = & x_{00}+x_{02}+x_{10}+x_{11}+x_{21}+x_{22} = d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{2}) = d(\underset{\sim}{a}+\underset{\sim}{2},\underset{\sim}{b}+\underset{\sim}{1}) \\ d(\underset{\sim}{a}+\underset{\sim}{2},\underset{\sim}{b}) & = & x_{00}+x_{01}+x_{11}+x_{12}+x_{20}+x_{22} = d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{1}) = d(\underset{\sim}{a}+\underset{\sim}{1},\underset{\sim}{b}+\underset{\sim}{2})\ . \end{array}$$

Further $d(\underset{\sim}{a},\underset{\sim}{b}) + d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{1}) + d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{2}) = 2\sum_{i=0}^{2}\sum_{j=0}^{2} x_{ij} = 2n\ .$ □

This allows us to readily test the distance of a constructed code, as in the following

LEMMA 10. *Suppose* A *is a ternary* (n,M,d)*-code then*

$$\begin{pmatrix} A \\ A+1 \\ A+2 \end{pmatrix}$$

is a ternary $(n,3M,d')$*-code where* $d' = \min\left(d(\underset{\sim}{a},\underset{\sim}{b}), d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{1}), 2n-d(\underset{\sim}{a},\underset{\sim}{b}) - d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{1})\right)$ $\underset{\sim}{a}, \underset{\sim}{b}$ *codewords of* A.

Example 1. Suppose $A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}$, a ternary $(5,6,4)$-code, then to find d' we merely need to test $\underset{\sim}{a} = (0,0,0,0,0)$ with $\underset{\sim}{b} = (0,1,2,2,1)$ which gives $d' = \min(4,3,3) = 3$ and $\underset{\sim}{a} = (0,1,2,2,1)$ with $\underset{\sim}{b} = (2,1,0,1,2)$ which gives $d' = \min(4,3,3) = 3$ giving a $(5,18,3)$-code.

THEOREM 3. *Let* A *be a ternary* $(n-1,M,d)$*-code. Further define*

$$d_1 = \min_{\underset{\sim}{a},\underset{\sim}{b}\in A} d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{1}) \quad \text{and} \quad d_2 = 2(n-1)-d-d_1 .$$

Then there exists ternary $(n,3M,\min(d,d_1+1,d_2+1))$ *and* $(n-1,3M,\min(d,d_1,d_2))$ *codes.*

Proof. We consider

$$\begin{pmatrix} 0 & \\ \vdots & A \\ 0 & \\ 1 & \\ \vdots & A+1 \\ 1 & \\ 2 & \\ \vdots & A+2 \\ 2 & \end{pmatrix} = \begin{pmatrix} N_0 \\ \\ N_1 \\ \\ N_2 \end{pmatrix}$$

Any two rows of N_0 have distance $\geq d$. By Lemma 9 any two rows of N_1 and N_2 also have distance $\geq d$. By the second part of Lemma 9 the distance between any two rows of $A+i$ and $A+j$, $i \neq j$, is d_1 or d_2 where $d+d_1+d_2 = 2(n-1)$. Hence the minimum distance between rows of N_i and N_j, $i \neq j$, is d_1+1 or $d_2+1 = 2(n-1)-d-d_1+1$. This gives the result.

Example 2.

$$A = \begin{pmatrix} 2 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 2 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 2 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 2 \end{pmatrix}$$

is a $(7,7,5)$-code with constant distance $d = 5$. Now $d_1 = 3$ and $d_2 = 6$. So in the Theorem

$$6n = 48 = 3(5+4+7) ,$$

giving a $(7,21,3)$ and $(8,21,4)$-code.

Example 3. For the $(13,13,9)$-code with constant distance $d = 9$. $d_1 = 10$ and $d_2 = 7$. So there exist $(13,39,7)$ and $(14,39,8)$-codes.

We can sometimes do better. We use

$$d_0 = \min d(\underset{\sim}{a},\underset{\sim}{b}), \quad d_1 = \min d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{1}), \quad d_2 = \min d(\underset{\sim}{a},\underset{\sim}{b}+\underset{\sim}{2}).$$

where $\underset{\sim}{a},\underset{\sim}{b}$ run over all vectors of the code.

THEOREM 4. *Let* A *be a ternary* (n,M,d) *code. Then there are ternary codes with parameters:*

i) $(2n,2M,\min(2d,2n-2))$, $(2n,3M,\min(2d,2n-d,2d_1))$

ii) $(2n, 9M, \min(n, 2d, d+d_1, 2n-d_1, 2n-d))$,

iii) $(3n, 9M, \min(3d, 3d_1, 2n-d, 2n-d_1))$.

Proof. i) With d_0, d_1, d_2 defined above, consider

$$\begin{pmatrix} A & A \\ A+1 & A+2 \end{pmatrix}, \quad \begin{pmatrix} A & A \\ A+1 & A+2 \\ A+2 & A+1 \end{pmatrix}.$$

The distances are $2d$, $d_1+d_2 = 2n-d$ respectively.

ii) Consider

$$\begin{pmatrix} A & A \\ A & A+1 \\ A & A+2 \\ A+1 & A \\ A+1 & A+1 \\ A+1 & A+2 \\ A+2 & A \\ A+2 & A+1 \\ A+2 & A+2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 2 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 2 & 0 \\ 2 & 1 \\ 2 & 2 \end{pmatrix} \circledast A$$

The distances are $2d$, n, $n+d_1$, $n+d_2$, $n+d$, $d+d_1$, $d+d_2$, d_1+d_2, $2n$. Since $d_i \le n$, we only need to consider n, $2d$, $d+d_1$, $2n-d_1$, $2n-d$.

iii) Let B be the $(3,9,2)$ ternary code. Consider $B \circledast A$ where $\circledast$ is defined in (ii). The distances are $3d$, d_i+d_j, $d+d_i$, $d+d_i+d_j$, $3n$, $3d_i$, $i,j = 1,2$. Now $d_i \le n$ and $d+d_i+d_j = 2n$, so we only need $3d$, $2n-d$, $2n-d_1$, $3d_1$, $6n-3d-3d_1$.

Example 4. Use $A = \begin{pmatrix} 0 & 0 \\ 1 & 2 \\ 2 & 1 \end{pmatrix}$ which is a $(2,3,2)$-code. Then E in is a $(4,27,2)$-code since $d = 2$, $n = 2$. C is a $(6,27,3)$-code.

$$C = [E\ F] = \left[\begin{array}{cccc|cc}
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 1 & 2 & 1 & 2 \\
2 & 1 & 2 & 1 & 2 & 1 \\
0 & 0 & 1 & 1 & 2 & 2 \\
1 & 2 & 2 & 0 & 0 & 1 \\
2 & 1 & 0 & 2 & 1 & 0 \\
0 & 0 & 2 & 2 & 1 & 1 \\
1 & 2 & 0 & 1 & 2 & 0 \\
2 & 1 & 1 & 0 & 0 & 2 \\
1 & 1 & 0 & 0 & 2 & 2 \\
2 & 0 & 1 & 2 & 0 & 1 \\
0 & 2 & 2 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 \\
2 & 0 & 2 & 0 & 2 & 0 \\
0 & 2 & 0 & 2 & 0 & 2 \\
1 & 1 & 2 & 2 & 0 & 0 \\
2 & 0 & 0 & 1 & 1 & 2 \\
0 & 2 & 1 & 0 & 2 & 1 \\
2 & 2 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 2 & 2 & 0 \\
1 & 0 & 2 & 1 & 0 & 2 \\
2 & 2 & 1 & 1 & 0 & 0 \\
0 & 1 & 2 & 0 & 1 & 2 \\
1 & 0 & 0 & 2 & 2 & 1 \\
2 & 2 & 2 & 2 & 2 & 2 \\
0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0
\end{array}\right]$$

Example 5. Using the (5,6,4)-code of Example 1 we have (10,18,6) and (10,54,5) ternary codes.

Corollary 11. *There exist ternary* $(2^{t+1}, 3.9^t, 2^t)$*-codes* $t \geq 1$.

Proof. Use the Theorem with the (4,27,2)-code of Example 4.

Codes with $d \le [\frac{2n}{3}]$

n	M(found)	M(max)	d	construction
3	9	9	9	Lemma 3
4	27		2	Example 4
5	18		3	Lemma 4
6	27		3	Example 4
6	18	18	4	Lemma 3
7	21		4	Corollary 6
8	27		5	From (9,27,6)-code
9	27	27	6	Lemma 3
10	54		5	Example 5
10	18		6	Twice (5,18,3)-code
11	36		7	From (12,36,8)-code
12	36	36	8	Lemma 3
13	39		7	Corollary 6
14	39		8	Example 3
15	18	45	10	(6,18,4) + (9,27,5)
16	54		10	From (17,54,10)-code
17	54		11	From (18,54,12)-code
18	54	54	12	Lemma 3
19	57		12	Corollary 6
20	21		13	From (21,21,14)-code
21	21	63	14	Corollary 6
22	36		14	Twice (11,36,7)-code
23	36		15	From (24,36,16)-code
24	36	72	16	Twice (12,36,8)-code
25	81		16	From (26,81,17)-code
26	81		17	From (27,81,18)-code
27	81	81	18	Lemma 3
28	36		18	From (29,36,20)-code
29	36		19	From (30,36,20)
30	36	90	20	(12,36,8) + (18,54,12)

Table 2

Levenshtein's Method:

Let us suppose that an arbitrary $GH(m,Z_3)$ exists, written on the additive group, whose first column is composed entirely of zero's: denote this matrix by M_m: and the matrix when is formed by stripping off the column of zero's by M_m'.

Example 6. $GH(6,Z_3) = M_6$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}$$

$$M_6' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{bmatrix}$$

The theory giving the construction of maximal codes requires matrices of particular orders and distances. The proofs of the following two lemmas are obvious:

LEMMA 12. *If there exists an* M_{3t} *(respectively* $M_{3(t+1)}$*) then the rows of* M_{3t}' *(respectively* $M_{3(t+1)}'$*) form a code with parameters* $n = 3t-1$, $M = 3t$, $d = 2t$ *(respectively* $n = 3t+2$, $M = 3(t+1)$, $d = 2(t+1)$*).*

Write

$$i = \left[\frac{d}{3d-2n}\right] . \tag{2}$$

LEMMA 13. *If* $3d > 2n \geq 2d$ *then there exist integers* a *and* b *such that*

$$\left.\begin{aligned} n &= a(3i-1) + b(3i+2) \\ d &= 2ai + 2b(i+1) \end{aligned}\right\} \qquad (3)$$

Proof. We can define i in terms of the following inequalities

$$\left(\frac{d}{3d-2n}\right) - 1 < i \le \left(\frac{d}{3d-2n}\right) \qquad (4)$$

that is

$$\frac{2n-2d}{3d-2n} < i \le \frac{d}{3d-2n} \; . \qquad (5)$$

Consider the left inequality

$$2n-2d < i(3d-2n)$$

which on rearranging gives

$$\frac{2(i+1)}{(3i+2)} < \frac{d}{n} \; . \qquad (6)$$

Consider the right inequality of (5)

$$i(3d-2n) \le d$$

which on rearranging gives

$$\frac{d}{n} \le \frac{2i}{(3i-1)} \; . \qquad (7)$$

Combining (6) and (7) we obtain

$$\frac{2(i+1)}{(3i+2)} < \frac{d}{n} \le \frac{2i}{(3i-1)} \qquad (8)$$

The two inequalities of (8) may be written in determinant form:

$$\begin{vmatrix} d & 2(i+1) \\ n & (3i+2) \end{vmatrix} > 0 = A \text{ say} \qquad (9)$$

$$\begin{vmatrix} n & (3i-1) \\ d & 2i \end{vmatrix} \ge 0 = B \text{ say} . \qquad (10)$$

Now suppose that both A and B are even. Then let

$$A = 2a$$

$$B = 2b$$

so (9) and (10) became

$$A = 2a = d(3i+2) - 2n(i+1) \tag{11}$$

$$B = 2b = 2ni - d(3i-1) \tag{12}$$

solving (11) and (12) for n and d yield the required results (3).

Note: requiring that A and B are even imposes only one condition, namely that d is also even, but in the case of ternary codes the distance is in fact even for maximal codes as then $3d = 2n$.

Following Levenshtein, we define the operation of adjunction of the matrices

$$X = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n_1} \\ X_{21} & X_{22} & \cdots & X_{2n_1} \\ \vdots & \cdot\cdot & & \cdot\cdot \\ X_{L_1 1} & X_{L_1 2} & \cdots & X_{L_1 n_1} \end{pmatrix}$$

and

$$Y = \begin{pmatrix} Y_{11} & Y_{12} & \cdots & Y_{1n_2} \\ Y_{21} & Y_{22} & \cdots & Y_{2n_2} \\ \vdots & \cdot\cdot & & \cdot\cdot \\ Y_{L_2 1} & Y_{L_2 2} & \cdots & Y_{L_2 n_2} \end{pmatrix}$$

as follows

$$X + Y = \begin{pmatrix} X_{11} & X_{12} \cdots & X_{1n_1} & Y_{11} & Y_{12} & \cdots & Y_{1n_2} \\ X_{21} & X_{22} \ldots & X_{2n_1} & Y_{21} & Y_{22} & \ldots & Y_{2n_2} \\ \vdots & \cdot\cdot & \cdot\cdot & \cdot\cdot & \cdot\cdot & & \cdot\cdot \\ X_{L1} & X_{L2} \cdots & X_{Ln_1} & Y_{L1} & Y_{L2} & \cdots & Y_{Ln_2} \end{pmatrix}$$

where $L = \min(L_1, L_2)$.

The operation of extension of a matrix X, r times, is defined as the result of the consecutive adjuction of r matrices X.

Note: If the rows of the matrix X form a code with the parameters n_1, d_1 and M_1, and the rows of a matrix Y form a code with the parameters n_2, d_2 and M_2, then the rows of the matrix $aX + bY$ where a and b are integer non-negative numbers, form a code with the parameters

$$n = an_1 + bn_1$$

$$d = ad_1 + bd_2$$

and

$$M = \min(M_1, M_2)$$

<u>THEOREM 5.</u> *If* d *is even and* $3d > 2n \geq 2d$ *then the following matrix* M *is maximal in that it meets the bound*

$$A(n,d) = 3\left[\frac{d}{3d-2n}\right] = 3i$$

$$M = aM'_{3i} + bM'_{3(i+1)}$$

$$a = \tfrac{1}{2}d(3i+2) - n(i+1)$$

$$b = ni - \tfrac{1}{2}d(3i-1) .$$

<u>*Proof.*</u> For the proof of the theorem, it is sufficient to see, using lemmas 12 and 13 that the above construction does indeed generate a maximal code.

<u>Example 7.</u> As an illustration, we present the maximal (13,6,10) code

$$\begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&2&2&1&1&2&0&1&2&0&1&2 \\ 1&0&1&2&2&2&1&0&2&1&0&2&1 \\ 2&1&0&1&2&0&0&1&1&1&2&2&2 \\ 2&2&1&0&1&1&2&1&2&0&2&0&1 \\ 1&2&2&1&0&2&1&1&0&2&2&1&0 \end{bmatrix}$$

Table 3 Examples of maximal ternary codes constructed using Theorem 5.

n	M	d	$i = [\frac{d}{3d-2n}]$	a	b	Construction
5	6	4	2	1	0	M_6'
7	3	6	1	1	1	$M_3'+M_6'$
8	9	6	3	1	0	M_9'
9	3	8	1	2	1	$2M_3'+M_6'$
10	6	8	2	2	0	$2M_6'$
11	12	8	4	1	0	M_{12}'
11	3	10	1	3	1	$3M_3'+M_6'$
12	3	10	1	1	2	$M_3'+2M_6'$
13	6	10	2	1	1	$M_6'+M_9'$
13	3	12	1	4	1	$4M_3'+M_6'$
14	15	10	5	1	0	M_{15}' Note: the code does <u>not</u> exist since M_{15} does <u>not</u> exist.
14	3	12	1	2	2	$2M_3'+2M_6'$
15	6	12	2	3	0	$3M_6'$
15	3	14	1	5	1	$5M_3'+M_6'$
16	9	12	3	2	0	$2M_9'$
16	3	14	1	3	2	$3M_3'+2M_6'$
17	18	12	6	1	0	M_{18}'
17	3	14	1	1	3	$M_3'+3M_6'$
17	3	16	1	6	1	$6M_3'+M_6'$

References

[1] I.F. Blake and R.C. Mullin, *An Introduction to Algebraic and Combinatorial Coding Theory*, Academic Press, New York, 1976.

[2] W. de Launey, Non-existence of generalized Hadamard matrices, *J. Stat. Planning and Inference*. (To appear).

[3] W. de Launey and J. Seberry, Generalized Bhaskar Rao designs with block size four. (To appear).

[4] D.A. Drake, Partial λ-geometries and generalized matrices over groups, *Canad. J. Math.* 31 (1979), 617-627.

[5] D. Jungnickel, On difference matrices, resolvable TD's and generalised Hadamard matrices, *Math. Z.* 167 (1979), 49-60.

[6] C. Lam and J. Seberry, Generalized Bhaskar Rao designs, *J. Stat. Planning and Inference*. (To appear).

[7] V.I. Levenshtein, Application of the Hadamard matrix to a problem of coding, *Problemy Kibernetiki*, 5(1961), 123-136.

[8] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Vol. 1, (North-Holland 1977).

[9] R. Mathon, private communication, 1983, gave us the BRD$(19,9,4;Z_2)$.

[10] D. Rajkundlia, Some techniques for constructing new infinite families of balanced incomplete block designs, *Discrete Math.* 44 (1983), 61-96.

[11] J. Seberry, A construction for generalized Hadamard matrices, *J. Stat. Planning and Inference*, 4(1980), 365-368.

[12] J. Seberry, Regular group divisible designs and Bhaskar Rao designs with block size three, *J. Stat. Planning and Inference*, (To appear).

[13] E. Seiden, As quoted by D.J. Street [14].

[14] D.J. Street, Generalized Hadamard matrices, orthogonal arrays and F-squares, *Ars Combinatoria*, 8(1979), 131-141.

[15] D.J. Street and C.A. Rodger, Some results on Bhaskar Rao designs *Combinatorial Mathematics III*. Lecture Notes in Mathematics, Vol. 829 (Springer-Verlag, 1980), 238-245.